PCT WELTORGANISATION FÜR GEISTIGES EIGENTUM
Internationales Büro

INTERNATIONALE ANMELDUNG VERÖFFENTLICHT NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT)

(51) Internationale Patentklassifikation 6 :		(11) Internationale Veröffentlichungsnummer: WO 96/22647
H04M 3/24, 15/28, 15/00	A1	(43) Internationales Veröffentlichungsdatum: 25. Juli 1996 (25.07.96)

(21) Internationales Aktenzeichen: PCT/EP96/00164

(22) Internationales Anmeldedatum: 17. Januar 1996 (17.01.96)

(30) Prioritätsdaten:
195 01 601.7 20. Januar 1995 (20.01.95) DE

(71)(72) Anmelder und Erfinder: BETH, Thomas [DE/DE]; Hohentwielweg 8, D-76377 Waldbronn (DE).

(72) Erfinder; und

(75) Erfinder/Anmelder *(nur für US)*: GEISELMANN, Willi [DE/DE]; Ostmarkstrasse 84c, D-76227 Karlsruhe (DE). KNOBLOCH, Hans-Joachim [DE/DE]; Oberkirchfeldstrasse 71, D-76135 Karlsruhe (DE). WICHMANN, Peer [DE/DE]; An der Sägmühle 6, D-75053 Gondelsheim (DE).

(74) Anwälte: LICHTI, Heiner usw.; Postfach 41 07 60, D-76207 Karlsruhe (DE).

(81) Bestimmungsstaaten: AU, JP, NO, US, europäisches Patent (AT, BE, CH, DE, DK, ES, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

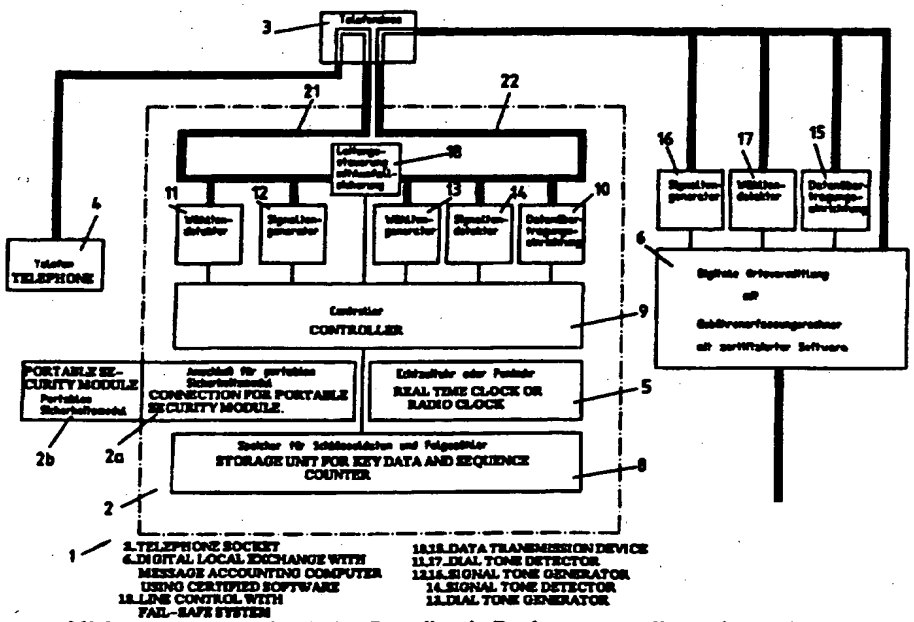
Veröffentlicht
Mit internationalem Recherchenbericht.

(54) Title: METHOD AND DEVICE FOR ENSURING RELIABLE COLLECTION OF DATA RELATING TO THE USE OF A COMMUNICATIONS SYSTEM

(54) Bezeichnung: VERFAHREN UND VORRICHTUNG ZUM SICHEREN ERFASSEN VON DATEN DER NUTZUNG EINES KOMMUNIKATIONSSYSTEMS

(57) Abstract

To ensure that a subscriber in a communications system is billed by the operator of the system only for actual use of the system and to allow detection of unauthorised access to the system, the invention proposes a method of ensuring reliable collection of data relating to the use of at least one such communications system by at least one first subscriber. The proposed method involves authentication of the data relating to the use of the system by the first subscriber in relation to the operator. A device of the type proposed is characterised by a security device connected to a terminal, the purpose of the security device being to authenticate data relating to the use of the communications system by the first subscriber in relation to the operator.



(57) Zusammenfassung

Um sicherzustellen, daß einem Teilnehmer eines Kommunikationssystems von einem Betreiber desselben nur die Kosten für die tatsächlichen Nutzungen durch den Betreiber in Rechnung gestellt werden und unzulässige Zugriffe auf das Kommunikationssystem erkannt werden, sieht die Erfindung ein Verfahren zum sicheren Erfassen von Daten der Nutzung mindestens eines solchen Kommunikationssystems mindestens durch einen ersten Teilnehmer vor, bei dem eine Authentifikation von Daten der Nutzung des Kommunikationssystems durch den ersten Teilnehmer gegenüber dem Systembetreiber erfolgt. Eine erfindungsgemäße Vorrichtung ist gekennzeichnet durch eine mit einem Endgerät verbundene Sicherheitseinrichtung zur Authentifikation von Daten der Nutzung des Kommunikationssystems durch den ersten Teilnehmer gegenüber dem Systembetreiber.

LEDIGLICH ZUR INFORMATION

Codes zur Identifizierung von PCT-Vertragsstaaten auf den Kopfbögen der Schriften, die internationale Anmeldungen gemäss dem PCT veröffentlichen.

AM	Armenien	GB	Vereinigtes Königreich	MX	Mexiko
AT	Österreich	GE	Georgien	NE	Niger
AU	Australien	GN	Guinea	NL	Niederlande
BB	Barbados	GR	Griechenland	NO	Norwegen
BE	Belgien	HU	Ungarn	NZ	Neuseeland
BF	Burkina Faso	IE	Irland	PL	Polen
BG	Bulgarien	IT	Italien	PT	Portugal
BJ	Benin	JP	Japan	RO	Rumänien
BR	Brasilien	KE	Kenya	RU	Russische Föderation
BY	Belarus	KG	Kirgisistan	SD	Sudan
CA	Kanada	KP	Demokratische Volksrepublik Korea	SE	Schweden
CF	Zentrale Afrikanische Republik	KR	Republik Korea	SG	Singapur
CG	Kongo	KZ	Kasachstan	SI	Slowenien
CH	Schweiz	LI	Liechtenstein	SK	Slowakei
CI	Côte d'Ivoire	LK	Sri Lanka	SN	Senegal
CM	Kamerun	LR	Liberia	SZ	Swasiland
CN	China	LK	Litauen	TD	Tschad
CS	Tschechoslowakei	LU	Luxemburg	TG	Togo
CZ	Tschechische Republik	LV	Lettland	TJ	Tadschikistan
DE	Deutschland	MC	Monaco	TT	Trinidad und Tobago
DK	Dänemark	MD	Republik Moldau	UA	Ukraine
EE	Estland	MG	Madagaskar	UG	Uganda
ES	Spanien	ML	Mali	US	Vereinigte Staaten von Amerika
FI	Finnland	MN	Mongolei	UZ	Usbekistan
FR	Frankreich	MR	Mauretanien	VN	Vietnam
GA	Gabon	MW	Malawi		

Verfahren und Vorrichtung zum sicheren Erfassen von Daten der Nutzung eines Kommunikationssystems

Die Erfindung betrifft ein Verfahren und eine Vorrichtung zum sicheren Erfassen von Daten der Nutzung mindestens eines Kommunikationssystems eines Systembetreibers mindestens durch einen ersten Teilnehmer, wobei die Vorrichtung ein Endgerät für den ersten Teilnehmer und eine Verbindung zum Kommunikationssystem aufweist.

Wenn ein erster Teilnehmer eines Kommunikationssystems, wie insbesondere eines Telefonnetzes, aber auch von Datenbanken oder dergleichen, die gegebenenfalls über ein solches Netz erreichbar sind, über das System mit einem anderen Teilnehmer kommuniziert, tritt bei der entgeltlichen oder kostenpflichtigen Nutzung des Kommunikationssystems das Problem auf, daß die Nutzung des Systems durch unberechtigte Dritte zu Lasten des Teilnehmers erfolgen kann, die sich beispielsweise auf die ungesicherte Verbindungsleitung des Teilnehmers zum Kommunikationssystem in einem Bereich aufschalten können, der außerhalb des Einflußbereiches des Teilnehmers liegt. Beispielsweise

können sich unberechtigte Dritte auf Telefonleitungen eines Teilnehmers aufschalten, insbesondere eine vom Teilnehmer erstellte Verbindung zu einer Ortsvermittlung durch Einschalten eines niederohmigen Abschlusses aufrechterhalten und für eigene Kommunikationen nutzen. Dies kann erhöhte Telefonrechnungen für einen Teilnehmer ergeben, aufgrund von Telefongesprächen, die er nicht geführt hat.

Aufgrund dieses Problems sollen für Teilnehmer Einzelabrechnungen erfolgen, die aber das Grundproblem der unberechtigten Nutzung nicht lösen, sondern für Teilnehmer und Systembetreiber bestenfalls nachträglich eine unzulässige Nutzung erkennbar machen; auch ergeben sich Probleme des Datenschutzes, auch wenn einige Endziffern der in der Einzelaufstellung enthaltenen angewählten Telefonnummern fortgelassen werden, wenn die entsprechenden Aufstellungen Mitbewohnern oder anderen Mitarbeitern zugänglich werden.

Der Erfindung liegt daher die Aufgabe zugrunde, unter Vermeidung der vorgenannten Nachteile ein Verfahren und eine Vorrichtung zum sicheren Erfassen von Daten der Nutzung eines Kommunikationssystems eines Systembetreibers durch einen Teilnehmer zu schaffen, die sowohl eine unberechtigte Nutzung vermeidet als auch für einen Teilnehmer die Nutzungsdaten korrekt und nachprüfbar erfaßt.

Erfindungsgemäß wird die genannte Aufgabe bei einem Verfahren der eingangs genannten Art dadurch gelöst, daß eine Authentifikation von Daten der Nutzung des Kommunikationssystems durch den ersten Teilnehmer gegenüber dem Systembetreiber erfolgt. Eine gattungsgemäße Vorrichtung ist zur Lösung der genannten Aufgabe dadurch gekennzeich-

net, daß mit dem Endgerät eine Sicherheitseinrichtung zur Authentifikation von Daten der Nutzung des Kommunikationssystems durch den ersten Teilnehmer gegenüber dem Systembetreiber verbunden ist.

Die Erfindung geht aus von mindestens einem Teilnehmer oder Kommunikationspartner, der mit einem anderen Informationen austauschen will, und einem Netzbetreiber, wobei zumindest der erste Teilnehmer Kosten trägt, die der Netzbetreiber für die Kommunikation in Rechnung stellt, wozu Nutzungsdaten erhoben werden müssen.

Daten der Nutzung des Kommunikationssystems oder kurz Nutzungsdaten können Daten über die Person des Teilnehmers - Teilnehmerdaten - und über die Verbindung - Verbindungsdaten - beinhalten, wie Zeit(punkt), Dauer, (Daten-)Volumen, Absender, Empfänger. Nutzungsdaten sind zu unterscheiden von Daten, die zwischen den Teilnehmern ausgetauschte Informationen beinhalten und oft als Nutzdaten bezeichnet werden.

Die Erfindung sichert zunächst die Authentizität des Teilnehmers gegenüber dem Netzbetreiber durch kryptographische Maßnahmen im Hinblick darauf, daß die Identifikation über die Anschlußleitung nicht sicher ist. Darüber hinaus gewährleistet sie eine auch durch Dritte überprüfbare Abrechnung des Netzbetreibers gegenüber dem Kommunikationspartner. Die Erfassung von Nutzungsdaten findet zwischen dem ersten Teilnehmer und dem für ihn zuständigen Netzbetreiber statt und ist in ihrer Form grundsätzlich unabhängig von den Eigenschaften der Kommunikationsverbindung.

Als Teilnehmerdaten kommen allgemein Daten in Frage, die in einer entsprechenden Sicherheitseinrichtung fest eingespeichert sind, oder Daten, die nur einem Teilnehmer zugänglich sind und durch diesen bei einer Verbindungsanforderung eingegeben werden können. Die Sicherheitseinrichtung kann in ein Telefon oder eine Nebenstellenanlage integriert sein, sie kann auch ein hiervon separates, zusätzliches Teil sein. Bei einer bevorzugten Ausgestaltung der erfindungsgemäßen Vorrichtung dahingehend, daß die Sicherheitseinrichtung einen Anschluß für ein portables Sicherheitsmodul aufweist, kann es sich bei den den Teilnehmer charakterisierenden, zur Durchführung der Authentifikation verwendeten Daten auch um in einem solchen Modul gespeicherte Teilnehmer-Daten handeln. Ein solches portables Sicherheitsmodul ist in der Regel als sogenannte Chip-Karte ausgeführt.

Authentifikation beinhaltet hierbei, daß die Sicherheitseinrichtung dem Kommunikationssystem bzw. dem Systembetreiber beweist, daß er eben der fragliche Teilnehmer ist und niemand sonst dem System beweisen kann, daß er der fragliche Teilnehmer ist, wobei je nach Ausgestaltung des Verfahrens nicht einmal der Systembetreiber selbst dies tun könnte. Geeignete Authentifikationsverfahren sind als solche bekannt.

Die bei solchen Authentifikationsverfahren erzeugten authentifizierenden Daten (Authentikatoren) sind beispielsweise: digitale Unterschriften (z.B. nach Digital Signature Standard), message authentification codes (z.B. nach Standard ISO 8731-2) oder Mischformen bzw. Abwandlungen davon.

Wesentlicher Kern der Erfindung ist, daß nicht nur der Teilnehmer gegenüber dem Kommunikationssystem authentifiziert wird, sondern darüber hinaus auch eine Authentifikation der Verbindungsdaten erfolgt, da andernfalls ein unberechtigter Dritter eine Verbindung in der schon oben beschriebenen Weise neu aufbauen könnte.

Die Authentifikation der Verbindungsdaten beinhaltet grundsätzlich die Authentifikation von Verbindungsaufbaudaten. Gemäß alternativer bevorzugter Ausgestaltungen kann darüber hinaus die Authentifikation von Verbindungsabbaudaten vorgesehen sein und/oder es kann vorgesehen sein, daß während der Verbindung vom Teilnehmer zum Kommunikationssystem Daten zur Authentifikation übertragen werden.

Werden vom berechtigten Teilnehmer Verbindungsabbaudaten an das Kommunikationssystem übertragen bzw. bricht die während einer Verbindung erfolgte Übertragung authentifizierter Daten ab, so erkennt das Kommunikationssystem, daß der berechtigte Teilnehmer seine Verbindung beendet hat und möglicherweise ein unberechtigter Teilnehmer die aufgebaute Verbindung zu nutzen versucht und kann daher die Verbindung seinerseits beenden.

Verbindungsaufbaudaten können ohne weiteres vor Herstellen der physikalischen Verbindungen zu einem gewünschten Zielteilnehmer an das Kommunikationssystem übermittelt werden. Wenn die Authentifikation von Verbindungsabbaudaten erfolgen soll, so kann in bevorzugter Ausgestaltung vorgesehen sein, daß nach Beendigung einer Nutzungsverbindung durch den Teilnehmer noch für eine vorgegebene kurze Zeit Verbindungsabbaudaten übermittelt werden, worauf eine Weiterbildung vorsieht, daß nach Übermittlung

von Verbindungsabbaudaten die Verbindung durch das Kommunikationssystem abgebaut wird. Um darüber hinaus Manipulationen am Rechner des Kommunikationssystems zu verhindern, erweitert sich der erfindungsgemäße Anspruch dahingehend, daß an dieser Stelle überprüfte, z.B. zertifizierte Software einzusetzen ist.

In diesem Falle sind keine aufwendigen vorrichtungsmäßigen Voraussetzungen erforderlich. Wenn Verbindungsdaten während der Teilnehmerverbindung an das Kommunikationssystem, wie eine Ortsvermittlungsstelle, übermittelt werden sollen, so kann dies in einem Telefonnetz per Einwegsignalisierung über Tonwahl im Rahmen des Mehrfrequenzwahlverfahrens (MFV) oder bei Zweiwegsignalisierung über Data-over-Voice-Technologie erfolgen. Dabei wird eine Datenübertragung z.B. in nicht genutzten Frequenzbereichen durchgeführt. Bei ISDN können Daten während der Nutzverbindung im Signalisierungskanal, wie dem D-Kanal, übertragen werden. In analoger Form können ebenfalls Verbindungsdaten sowie Authentifikatoren vom Kommunikationssystem zum Benutzer übertragen werden, wobei insbesondere im Fall, daß dies von der Ortsvermittlungsstelle passiert, ohne Schwierigkeiten z.B. in Gebührenimpulsen codierte Information übertragen werden kann.

Gemäß einer bevorzugten Weiterbildung kann vorgesehen sein, daß die Zahl der Nutzungen teilnehmerseitig gezählt wird und die der jeweiligen Nutzung entsprechende Zahl in die Authentifikation eingeht. Hierdurch wird vermieden, daß ein unberechtigter Dritter Verbindungsdaten, wie insbesondere Verbindungsaufbaudaten, abfängt und zur Erzeugung einer unberechtigten erneuten Verbindung nutzt; in weiterer bevorzugter Ausgestaltung kann vorgesehen sein, daß während der Verbindung ansteigende Zähl-Daten

verschlüsselt übertragen werden. Hierdurch wird verhindert, daß ein unberechtigter Dritter während der Verbindung übertragene Daten abfängt und nach Beendigung der berechtigten Verbindung zur Aufrechterhaltung einer eigenen gewünschten Verbindung benutzt. Das erfindungsgemäße Verfahren sieht nämlich weiterhin vor, daß das Kommunikationssystem die Verbindung beendet, wenn es keine oder falsche Authentifikations- oder Zähl-Daten empfängt. Während es grundsätzlich möglich ist, daß Nutzungsdaten nur durch das Kommunikationssystem erfaßt werden, sieht eine äußerst bevorzugte Weiterbildung vor, daß auch teilnehmerseitig Nutzungsdaten erfaßt werden. In diesem Falle können die teilnehmerseitig erfaßten Nutzungsdaten an das Kommunikationssystem übermittelt und mit den dort erfaßten Nutzungsdaten verglichen werden, so daß sogleich nach Beendigung einer berechtigten Teilnehmerverbindung eine Überprüfung und ein Abgleich erfolgen kann. Im Falle der Zweiwegsignalisierung erfolgt eine gegenseitige Signalisierung und ein Abgleich.

In bevorzugter Ausgestaltung kann vorgesehen sein, daß vom Kommunikationssystem Informationen zur Bestimmung von Nutzungsdaten an den Teilnehmer übermittelt werden. Im Rahmen eines Telefonnetzes als Kommunikationssystem handelt es sich bei den fraglichen Informationen in der Regel um nicht bekannte Gebührenimpulse, die insbesondere auch authentifiziert zum Teilnehmer übertragen werden können. Die erfindungsgemäße Vorrichtung sieht in diesem Falle vor, daß die Sicherheitseinrichtung eine Einheit zum Empfang und zur Verarbeitung von Nutzungs-Informationen aufweist. Alternativ kann zur teilnehmerseitigen Berechnung von Nutzungsdaten vorgesehen sein, daß die Sicherheitseinrichtung eine Echtzeituhr oder aber eine Funkuhr aufweist. In letzterem Falle wird die Sicherheit

des Kommunikationssystems bzw. seines Systembetreibers gegenüber Manipulationen durch den Teilnehmer in bevorzugter Ausgestaltung dadurch gewährleistet, daß die Zeitimpulse für die Funkuhr an diese mit einem Authentikator versehen übermittelt werden.

In weiterer bevorzugter Ausgestaltung kann vorgesehen sein, daß Nutzungsdaten teilnehmerseitig gespeichert werden und daß Nutzungsdaten teilnehmerseitig angezeigt werden, wobei insbesondere die Nutzungsdaten verschlüsselt werden, so daß diese nur ein berechtigter Teilnehmer, der einen entsprechenden Schlüssel besitzt, in Klarschrift lesen kann, womit verhindert wird, daß unberechtigte Dritte die Nutzungsdaten in Klarschrift zur Kenntnis nehmen.

Während die Erfindung grundsätzlich davon ausgeht, daß neben Teilnehmerdaten auch Verbindungsdaten vom Teilnehmer zum Kommunikationssystem übermittelt werden, kann in bevorzugter Ausgestaltung ebenfalls vorgesehen sein, daß das Kommunikationssystem sich gegenüber dem Teilnehmer authentifiziert.

Der Aufbau der Nutzverbindung kann erst nach erfolgter Eingabe der Wählinformation durch den Teilnehmer erfolgen; die Beendigung der Eingabe der Wählinformation kann in einfachster Weise dadurch angezeigt werden, daß das Wählen mit einem Endezeichen, beispielsweise dem bei einem Telefon vorgesehenen "*" (einem Stern), beendet wird. Alternativ kann vorgesehen sein, daß der Aufbau einer Nutzverbindung durch die Sicherheitseinrichtung zur Zeit der Eingabe der Wählinformation vom Teilnehmer erfolgt. In diesem Falle fügt die Sicherheitseinrichtung

die Authentifikationsdaten in eine zeitlich gespreizte Absendung der Wählsignale ein.

Wenn ein portables Sicherheitsmodul, wie eine Chip-Karte, verwendet wird, so kann weiterhin vorgesehen sein, daß in diesem durch geeignete externe Einrichtungen Kommunikationsgebühren eingespeichert werden, so daß sogleich eine Abrechnung der Kommunikationskosten nach Beendigung der Verbindung durch das portable Sicherheitsmodul erfolgen kann.

Die Sicherheitseinrichtung kann neben der Authentifikation auch zum Erbringen zusätzlicher Sicherheitsfunktionen dienen, wie beispielsweise einer Verschlüsselung der Kommunikation; weiterhin kann sie mit einer Sprachausgabe versehen sein.

Die Erfindung ist nicht nur einsetzbar bei der Nutzung eines einzigen Netzes eines einzigen Netzbetreibers durch den Teilnehmer, sondern auch wenn der Teilnehmer über das Netz eines ersten Netzbetreibers zu Netzen eines oder weiterer Betreiber eine Verbindung durchführt.

Weitere Vorteile und Merkmale der Erfindung ergeben sich aus den Ansprüchen und aus der nachfolgenden Beschreibung, in der ein Ausführungsbeispiel der Erfindung unter Bezugnahme auf die Zeichnung im einzelnen erläutert ist. Dabei zeigt:

Fig. 1 eine schematische Darstellung der bevorzugten Ausgestaltung der erfindungsgemäßen Vorrichtung zur sicheren

Erfassung von Daten der Nutzung eines Kommunikationssystems; und

Fig. 2 ein eine bevorzugte Ausgestaltung des erfindungsgemäßen Verfahrens darstellendes Ablaufdiagramm.

Die erfindungsgemäße Vorrichtung 1 zur sicheren Erfassung von Daten der Nutzung eines Kommunikationssystems weist zunächst eine Sicherheitseinrichtung 2 auf. Im dargestellten Ausführungsbeispiel ist die Sicherheitseinrichtung 2 teilnehmerseitig mit einer Telefondose 3 verbunden. Es kann sich hierbei um eine Telefondose für ein analoges Telefon 4 handeln, wie sie derzeit als TAE-Dose realisiert ist; die Telefondose 3 kann auch eine Telefondose für ein digitales Telefonsystem, ein ISDN-System, sein. Über die Telefondose 3 erfolgt die Verbindung zu einer digitalen Ortsvermittlung 6 mit einem Gebührenerfassungsrechner als Teil der Kommunikationseinrichtung des Systembetreibers, der im dargestellten Ausführungsbeispiel der Betreiber des entsprechenden Telefonsystems ist.

Bei dem Telefon 4 handelt es sich in der Regel um ein Tastaturtelefon mit einer Telefontastatur, wobei das Telefon in der Regel im Mehrfrequenzwählverfahren (MFV) betrieben wird, womit üblicherweise die Steuerung von Geräten möglich ist.

Bei der Sicherheitseinrichtung 2 handelt es sich im dargestellten Ausführungsbeispiel um ein dem Telefon 4 vorgeschaltetes Gerät. Die Sicherheitseinrichtung 2 weist einen Anschluß 2a auf, durch den ein portables Sicher-

heitsmodul 2b angeschlossen werden kann, in dem geheime Teilnehmerdaten gespeichert und gegebenenfalls bearbeitet werden können. Beim Sicherheitsmodul 2b kann es sich konkret um eine sogenannte Chip-Karte mit eigenem Prozessor handeln. In diesem Falle ist der Anschluß 2a als schlitzförmige Aufnahme für die Chip-Karte ausgebildet. Alternativ könnten auch sämtliche zur Durchführung des Verfahrens erforderlichen Einheiten, insbesondere die geheimen Teilnehmerdaten und eine Einrichtung zur Bearbeitung derselben in einer stationären Sicherheitseinrichtung 2 selbst integriert sein.

Die Sicherheitseinrichtung 2 weist einen nicht flüchtigen Speicher 8 auf; im Speicher sind die die Teilnehmerstelle (das Telefon 4) bzw. allgemein den Teilnehmer charakterisierenden Schlüsseldaten gespeichert. Weiterhin sind Folgezähldaten gespeichert. Es kann sich um solche handeln, die die Anzahl der getätigten Anrufe charakterisieren, oder auch zusätzlich kann es sich um Zähldaten handeln, die bei wiederholter Übermittlung von Informationen durch die Sicherheitseinrichtung an das Kommunikationssystem die Anzahl der getätigten Übermittlungen charakterisieren.

In der Sicherheitseinrichtung 2 ist weiterhin eine Uhr 5, wie eine Echtzeituhr oder eine Funkuhr, integriert. Hierdurch können beim Verbindungsauf- und/oder Verbindungsabbau zusätzlich die Dauer der bestehenden Verbindungen und/oder die aktuelle Uhrzeit mitübertragen werden.

Die Sicherheitseinrichtung 2 weist weiterhin einen Controller 9 auf, dessen wesentliches Element ein Mikroprozessor ist. Mit dem Controller 9 sind ein Wähltondetektor

11, ein Signaltongenerator 12, ein Wähltongenerator 13, eine Leitungssteuerung 18 und ein Signaltondetektor 14 verbunden.

Die Leitungssteuerung 18 stellt fest, wenn vom Telefon 4 eine Verbindungsanforderung erfolgt, also der Telefonhörer abgehoben ist und meldet dies an den Controller 9, der wiederum die Leitungssteuerung 18 veranlaßt, die Amtsleitung zu belegen. Der Wähltondetektor 11 stellt fest, wenn über die Tastatur ein Ziel-Teilnehmer angewählt wird und damit Wähltöne erzeugt werden. Der Wähltondetektor 11 meldet dies dem Controller 9. Nach der im weiteren zu erläuternden Überprüfung veranlaßt der Controller 9 den Wähltongenerator 13, in Wähltöne codierte Information weiter an die digitale Ortsvermittlung 6 zu senden.

Der Signaltondetektor 14 wiederum stellt von der digitalen Ortsvermittlung 6 ankommende Signaltöne, wie Freizeichen, Rufton, Besetztzeichen, Gebührenimpulse, fest, die der Controller 9 nach Überprüfung über den Signaltongenerator 12 an den Telefonhörer des Telefons 4 weitervermittelt.

Entsprechend sind der digitalen Ortsvermittlung 6 ein Signaltongenerator 16 und ein Wähltondetektor 17 vorgeschaltet.

Die Sicherheitseinrichtung 2 und die digitale Ortsvermittlung 6 weisen je eine Datenübertragungseinrichtung 10, 15, beispielsweise in Form eines sogenannten Data-over-Voice-Modems, auf, mit der je nach Ausprägung Daten auch gleichzeitig mit der Nutzverbindung zwischen Sicher-

heitseinrichtung 2 und Ortsvermittlung 6 übertragen werden können.

Um unabhängig von jeder Authentifikation und insbesondere auch bei Ausfall der Sicherheitseinrichtung 2 aufgrund einer Störung, beispielsweise eines Stromnetzausfalles, das Anwählen von Notruf- und gebührenfreien Nummern durch das Telefon 4 zu ermöglichen, ist weiterhin eine Leitungssteuerung 18 mit einer Ausfallsicherung vorgesehen; tritt eine solche Störung auf, so schaltet die Leitungssteuerung mit Ausfallsicherung die vom Telefon 4 kommende Leitung 21 zur Sicherheitseinrichtung 2 zu der zur Ortsvermittlung hin führenden Ausgangsleitung 22 durch.

Der Ablauf einer bevorzugten Ausgestaltung des erfindungsgemäßen Verfahrens wird im folgenden anhand der Figur 2 erläutert.

Im Rahmen der erfindungsgemäßen Vorrichtung arbeiten dabei die Sicherheitseinrichtung und die Vermittlung (digitale Ortsvermittlung 6 in Fig. 1) miteinander zusammen. Bei einer bevorzugten Ausgestaltung des erfindungsgemäßen Verfahrens dahingehend, daß dazu zertifizierte Software in der digitalen Ortsvermittlung verwendet wird, wird zusätzlicher Schutz gegen Manipulation durch Mitarbeiter des Systembetreibers erreicht.

Nimmt ein Nutzer den Telefonhörer 4 ab, so erfolgt hierdurch vom Telefon 4 eine Verbindungsanforderung an die Sicherheitseinrichtung 2, woraufhin in einem ersten Schritt S1 diese die Verbindungsanforderung erkennt und hierauf mit S2 eine Verbindung zur Vermittlung 6 herstellt. Nach Erkennung des von dieser erzeugten Freizei-

chens (S3) speichert die Sicherheitseinrichtung zunächst die von der Tastatur erzeugten Wählzeichen (S4).

In einem weiteren Schritt S5 generiert der Controller 9 der Sicherheitseinrichtung 2 aus den im Speicher gespeicherten Zähl- und Schlüsseldaten einen Authentikator, erhöht den Zähler im Speicher 8 und sendet den erzeugten Authentikator sowie die zwischengespeicherten Wählzeichen mit einem diesem zugeordneten Authentikator an die Vermittlung 6.

Diese überprüft Authentikator und Unterschrift und stellt bei Korrektheit den Verbindungsanruf zu dem gewünschten Ziel bzw. Ziel-Teilnehmer her und erzeugt einen Rufton.

Falls Authentikator oder Unterschrift falsch sind, so wird die Verbindungsanforderung zurückgewiesen, es sei denn, es wurde eine gebührenfreie Rufnummer angewählt. Erforderlichenfalls kann an die Sicherheitseinrichtung ein Fehlersignal gemeldet werden, das diese gegebenenfalls an den Teilnehmer weitergibt (Schritt S6).

Die Sicherheitseinrichtung 2 detektiert den Rufton im Schritt S7 und schaltet nach Herstellen der Verbindung diese zum Telefon 4 durch.

Bei der dargestellten Ausführungsform erzeugt die Vermittlung 6 während des gehaltenen Gesprächs in an sich bekannter Weise Gebührenimpulse, die der Sicherheitseinrichtung 2 als Nutzungsdaten übermittelt werden; diese zählt die Gebührenimpulse (S8).

Wenn durch den das Telefon 4 benutzenden Teilnehmer das Gespräch beendet wird, indem dieser den Hörer auflegt, so

erkennt die Sicherheitseinrichtung 2 dies; sie hält die Verbindung zur Ortsvermittlung 6 noch für eine kurze Zeit aufrecht, berechnet einen Abschlußauthentikator, der die angerufene Telefonnummer, die gezählten Gebührenimpulse, die hieraus berechnete Gesprächsdauer sowie einen Authentikator enthält, und sendet diese Daten an die Ortsvermittlung 6 (S9). Diese überprüft schließlich (S10) die empfangenen Daten einschließlich dem Authentikator auf ihre Richtigkeit und speichert die Daten; bei Bedarf gibt sie eine Alarmmeldung aus.

Patentansprüche

1. Verfahren zum sicheren Erfassen von Daten der Nutzung mindestens eines Kommunikationssystems eines Systembetreibers mindestens durch einen ersten Teilnehmer, wobei eine Authentifikation von Daten der Nutzung des Kommunikationssystems durch den ersten Teilnehmer gegenüber dem Systembetreiber erfolgt.

2. Verfahren nach Anspruch 1, gekennzeichnet durch Authentifikation von Verbindungsabbaudaten.

3. Verfahren nach einem der vorangehenden Ansprüche, dadurch gekennzeichnet, daß die Zahl der Nutzungen teilnehmerseitig gezählt wird und die der jeweiligen Nutzung entsprechende Zahl mitübertragen wird.

4. Verfahren nach Anspruch 2, dadurch gekennzeichnet, daß nach Beendigung einer Nutzungsverbindung durch den Teilnehmer noch für eine vorgegebene kurze Zeit Verbindungsabbaudaten übermittelt werden.

5. Verfahren nach Anspruch 2 oder 4, dadurch gekennzeichnet, daß nach Übermittlung von Verbindungsabbaudaten die Verbindung durch das Kommunikationssystem abgebaut wird.

6. Verfahren nach einem der vorangehenden Ansprüche, dadurch gekennzeichnet, daß während der Verbindung vom Teilnehmer zum Kommunikationssystem Daten zur Authentifikation übertragen werden.

7. Verfahren nach Anspruch 5, dadurch gekennzeichnet, daß während der Verbindung ansteigende Zähl-Daten verschlüsselt übertragen werden.

8. Verfahren nach Anspruch 5 oder 6, dadurch gekennzeichnet, daß das Kommunikationssystem die Verbindung beendet, wenn es keine oder falsche Authentifikations- oder Zähl-Daten empfängt.

9. Verfahren nach einem der vorangehenden Ansprüche, dadurch gekennzeichnet, daß teilnehmerseitig Nutzungsdaten erfaßt werden.

10. Verfahren nach einem der vorangehenden Ansprüche, dadurch gekennzeichnet, daß durch das Kommunikationssystem Nutzungsdaten erfaßt werden.

11. Verfahren nach Anspruch 6 und 7, dadurch gekennzeichnet, daß teilnehmerseitig erfaßte Nutzungsdaten an das Kommunikationssystem übermittelt und dort mit den dort erfaßten Nutzungsdaten verglichen werden.

12. Verfahren nach einem der vorangehenden Ansprüche, dadurch gekennzeichnet, daß vom Kommunikationssystem

Informationen zur Bestimmung von Nutzungsdaten an den Teilnehmer übermittelt werden.

13. Verfahren nach einem der vorangehenden Ansprüche, dadurch gekennzeichnet, daß Nutzungsdaten teilnehmerseitig gespeichert werden.

14. Verfahren nach einem der vorangehenden Ansprüche, dadurch gekennzeichnet, daß Nutzungsdaten teilnehmerseitig angezeigt werden.

15. Verfahren nach Anspruch 10 oder 11, dadurch gekennzeichnet, daß die Nutzungsdaten verschlüsselt werden.

16. Vorrichtung zur sicheren Erfassung von Daten der Nutzung mindestens eines Kommunikationssystems eines Systembetreibers mindestens durch einen ersten Teilnehmer, mit einem Endgerät für den ersten Teilnehmer und einer Verbindung zum Kommunikationssystem, wobei mit dem Endgerät (4) eine Sicherheitseinrichtung (2) zur Authentifikation von Daten der Nutzung des Kommunikationssystems durch den ersten Teilnehmer gegenüber dem Systembetreiber verbunden ist.

17. Vorrichtung nach Anspruch 16, dadurch gekennzeichnet, daß die Sicherheitseinrichtung (2) einen Anschluß für ein portables Sicherheitsmodul aufweist.

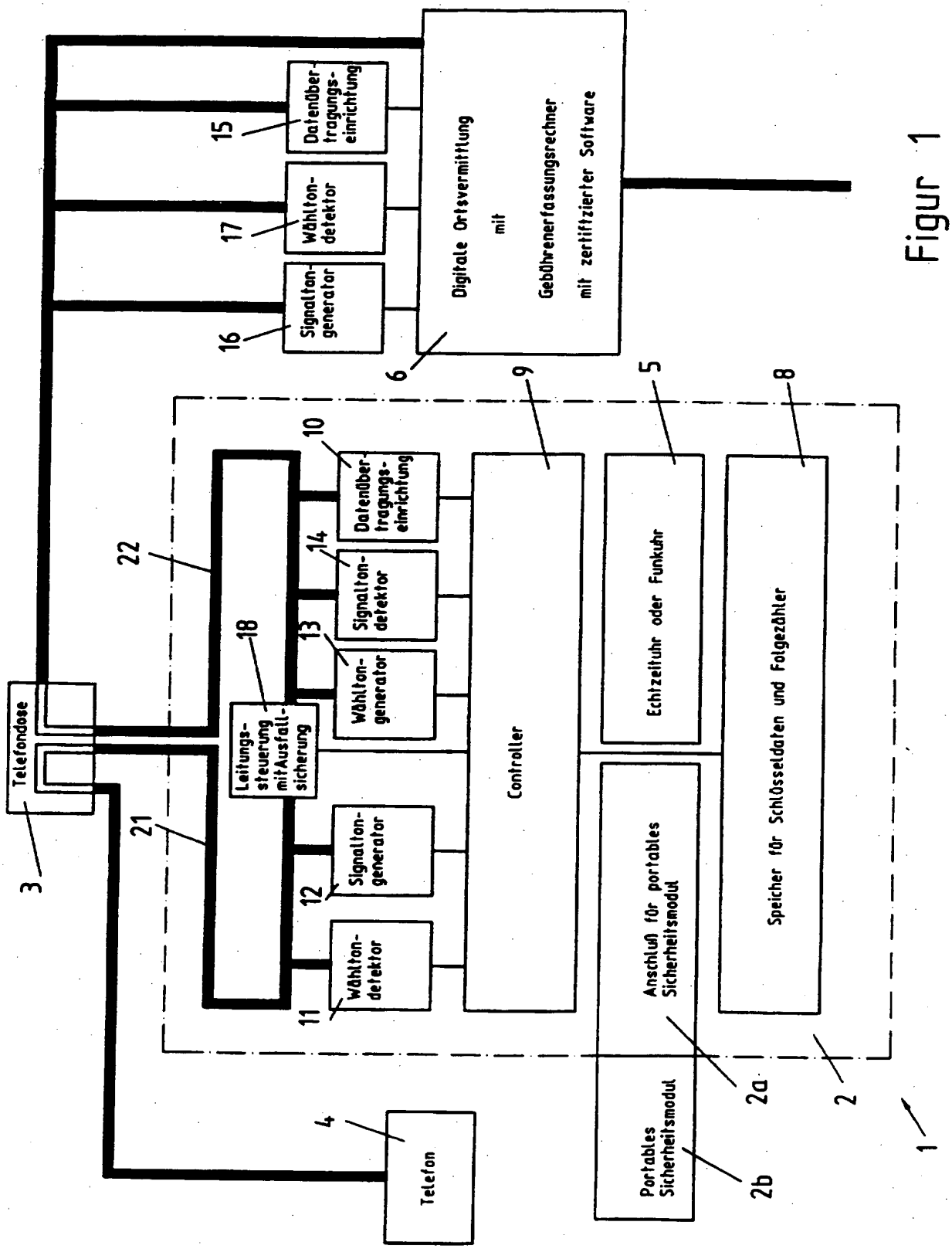
18. Vorrichtung nach Anspruch 16 oder 17, dadurch gekennzeichnet, daß die Sicherheitseinrichtung (2) eine Einheit zum Erkennen eines die Eingabe von Teilnehmerdaten anzeigenden Endzeichens aufweist.

19. Vorrichtung nach einem der Ansprüche 16 bis 18, dadurch gekennzeichnet, daß die Sicherheitseinrichtung (2) eine Einheit zum Empfang und zur Verarbeitung von Nutzungsinformationen aufweist.

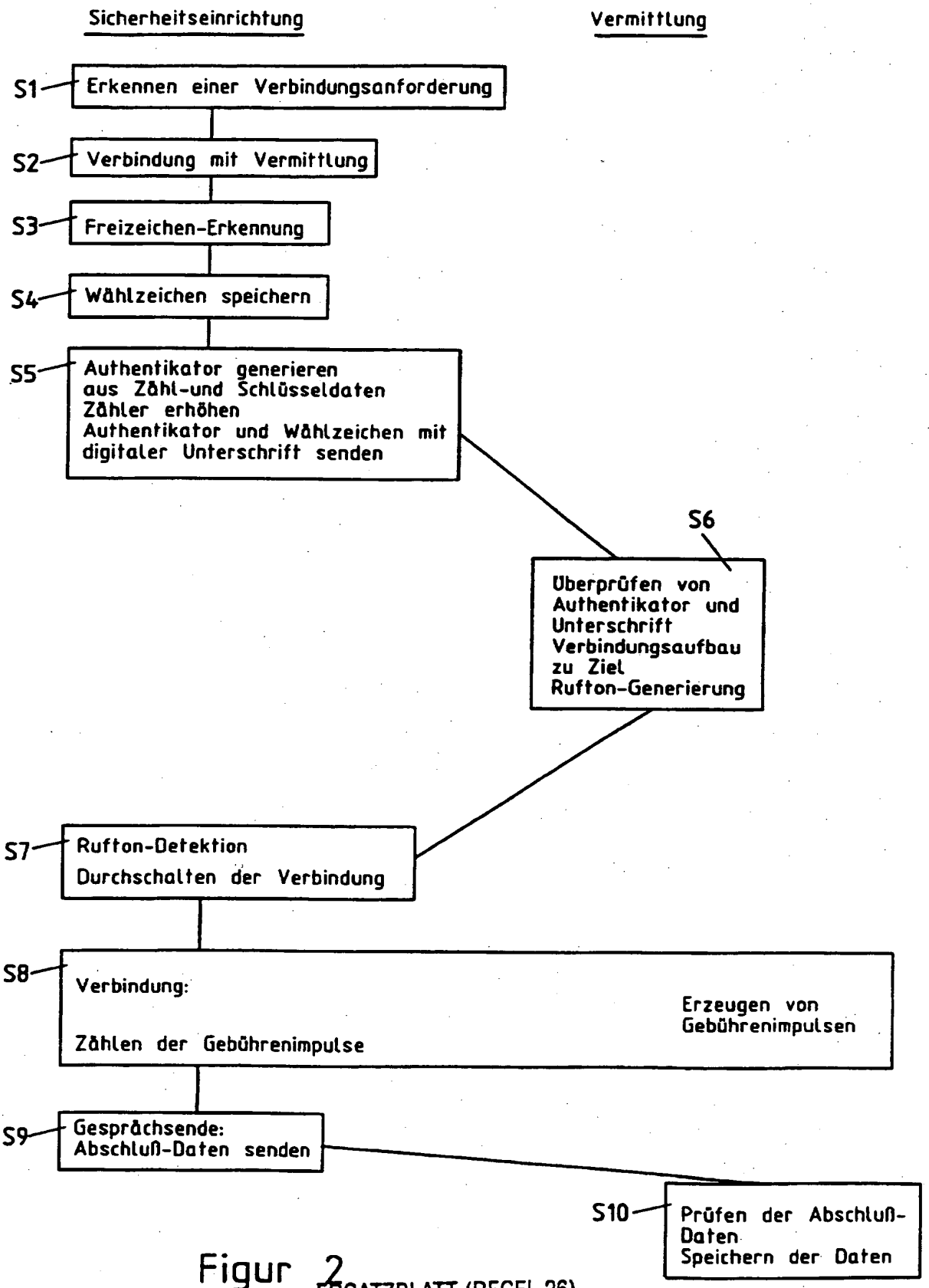
20. Vorrichtung nach einem der Ansprüche 16 bis 18, dadurch gekennzeichnet, daß die Sicherheitseinrichtung (2) eine Echtzeituhr aufweist.

21. Vorrichtung nach einem der Ansprüche 16 bis 18, dadurch gekennzeichnet, daß die Sicherheitseinrichtung (2) eine Funkuhr aufweist.

22. Vorrichtung nach einem der Ansprüche 16 bis 21, gekennzeichnet durch einen die Nutzungs-Verbindungen zählenden Zähler.


Digitale Ortsvermittlung
mit
Gebührenerfassungsrechner
mit zertifizierter Software
6
Datenüber-tragungs-einrichtung
15
Wählton-detektor
17
Signalton-generator
16
Datenüber-tragungs-einrichtung
10
Signalton-detektor
14
Wählton-generator
13
Leitungs-steuerung mit Ausfall-sicherung
18
Signalton-generator
12
Wählton-detektor
11
Controller
9
Echtzeituhr oder Funkuhr
5
Speicher für Schlüsseldaten und Folgezähler
8
Anschluß für portables Sicherheitsmodul
2a
Portables Sicherheitsmodul
2b
Telefondose
3
Telefon
4
22
21
2
1

Figur 1


Sicherheitseinrichtung
Vermittlung
S1
Erkennen einer Verbindungsanforderung
S2
Verbindung mit Vermittlung
S3
Freizeichen-Erkennung
S4
Wählzeichen speichern
S5
Authentikator generieren
aus Zähl-und Schlüsseldaten
Zähler erhöhen
Authentikator und Wählzeichen mit
digitaler Unterschrift senden
S6
Überprüfen von
Authentikator und
Unterschrift
Verbindungsaufbau
zu Ziel
Rufton-Generierung
S7
Rufton-Detektion
Durchschalten der Verbindung
S8
Verbindung:
Erzeugen von
Gebührenimpulsen
Zählen der Gebührenimpulse
S9
Gesprächsende:
Abschluß-Daten senden
S10
Prüfen der Abschluß-
Daten
Speichern der Daten

Figur 2

INTERNATIONAL SEARCH REPORT

Inter nal Application No
PCT/EP 96/00164

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 H04M3/24 H04M15/28 H04M15/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 H04M

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP,A,0 335 768 (SCHLUMBERGER INDUSTRIES) 4 October 1989 see column 3, line 25 - line 56	1,16
A	EP,A,0 200 847 (SODECO SAIA AG) 12 November 1986	

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
23 April 1996	09. 05. 96

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+ 31-70) 340-2040, Tx. 31 651 epo nl, Fax (+ 31-70) 340-3016	Vandevenne, M

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Inter nal Application No
PCT/EP 96/00164

Patent document cited in search report	Publication date	Patent family member(s)		Publication date
EP-A-335768	04-10-89	FR-A-	2629296	29-09-89
		DE-D-	68912957	24-03-94
		DE-T-	68912957	16-06-94
		JP-A-	2015739	19-01-90
		US-A-	5086457	04-02-92
EP-A-200847	12-11-86	CH-A-	668151	30-11-88

INTERNATIONALER RECHERCHENBERICHT

Inter nales Aktenzeichen
PCT/EP 96/00164

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 6 H04M3/24 H04M15/28 H04M15/00

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
IPK 6 H04M

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	EP,A,0 335 768 (SCHLUMBERGER INDUSTRIES) 4.Oktober 1989 siehe Spalte 3, Zeile 25 - Zeile 56 ---	1,16
A	EP,A,0 200 847 (SODECO SAIA AG) 12.November 1986 -----	

☐ Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

☒ Siehe Anhang Patentfamilie

* Besondere Kategorien von angegebenen Veröffentlichungen :

"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist

"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist

"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)

"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht

"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist

"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist

"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden

"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist

"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
23.April 1996	09.05.96

Name und Postanschrift der Internationale Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Vandevenne, M

INTERNATIONALER RECHERCHENBERICHT

Internales Aktenzeichen
PCT/EP 96/00164

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie		Datum der Veröffentlichung
EP-A-335768	04-10-89	FR-A-	2629296	29-09-89
		DE-D-	68912957	24-03-94
		DE-T-	68912957	16-06-94
		JP-A-	2015739	19-01-90
		US-A-	5086457	04-02-92
EP-A-200847	12-11-86	CH-A-	668151	30-11-88